

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
rfiem131@comcast.net

THAT IS STORED AT PREMISES
CONTROLLED BY COMCAST
CORPORATION

Magistrate No. 23-665
[Under Seal]

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Steven Adams, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with an account that is stored at premises controlled by Comcast Corporation (“Comcast”). The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Comcast to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent with the Department of Defense- Office of Inspector General’s Defense Criminal Investigative Service (DCIS) and have been since 2019. I am currently assigned to the Pittsburgh Resident Agency and handle cases involving procurement fraud, health care fraud, and other crimes against the Department of Defense.

3. Prior to serving as a DCIS Special Agent, I was a Special Agent with the Naval Criminal Investigative Service (NCIS), starting in 2006. During my tenure as an agent, I have participated in numerous criminal and national security investigations. My training and experience includes investigations of complex financial crimes, product substation, health care fraud, and money laundering, as well as foreign counterintelligence, economic espionage, and counter-proliferation.

4. As a Special Agent, I have assisted or participated in multiple investigations related to complex financial crimes. To successfully conduct these investigations, I have utilized or assisted in utilizing a variety of investigative techniques and resources, including the execution of search warrants, undercover operations, physical and electronic surveillance, subpoenas, criminal record and database queries, confidential sources, informants and other techniques. My training, experience and conversations with other special agents and law enforcement personnel has helped me become familiar with the methods and techniques utilized by white collar criminals; which has been useful and relevant during this investigation. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. The information contained in this affidavit is either personally known to me, based upon my interview of various witnesses and review of various records and publicly available information, or has been relayed to me by other agents or sworn law enforcement personnel. Because this affidavit is being submitted for the limited purpose of obtaining a search warrant for an email account, I have not included each and every fact known to me concerning the investigation. I have set forth only those facts that I believe are necessary to establish probable cause to support the requested search warrant.

6. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18 U.S.C. § 1343 (Wire fraud), 18 U.S.C. § 287 (False, fictitious or fraudulent claims) and 18 U.S.C. § 1031 (Major fraud against the United States) have been committed by Rena Turner and others. For reasons set forth below, I believe probable cause exists to search the email information described in Attachment A for evidence, instrumentalities, contraband or fruits of these crimes further described in Attachment B.

JURISDICTION

7. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

8. Law enforcement is investigating whether Rena Turner, through Gold Peak Industries (Gold Peak), falsely represented the source and description of products provided to the Defense Logistics Agency (DLA) under federal contracts.

9. DLA is the Department of Defense’s (DoD) combat logistics support agency, which means that it manages DoD’s supply chain, delivering spare parts and consumable supplies to DoD components all over the world. DLA is divided into a number of components, including DLA Construction and Equipment. DLA purchases many of its supplies from vendors. Each type of part ordered is identified by a unique number called a National Stock Number (NSN), which has unique specifications and/or drawings for form, fit and function.

10. When DLA issues a solicitation for a NSN, vendors respond with a quote that includes the sales price, the NSN to be provided, and references to applicable specifications/standards or drawings associated with the NSN. The vendor's quote will also include the Commercial and Government Entity (CAGE) code for the business where they will procure the product to be delivered to DLA.

11. The vendor is bound by contract to provide the material from the source listed on the quote and, if they deviate from that source, they are required to get approval from the contracting officer before shipping the material. Under normal circumstances, product received from vendors is not subject to a quality inspection to confirm it meets the NSN specifications or drawings. Instead, due to the high volume of material received, DLA relies on the integrity of its vendors to adhere to contract requirements.

12. This investigation was initiated based upon notification from DLA Office of Counsel that Gold Peak, located in Washington, PA, sold defective parts to DLA.

13. In August 2019, DLA Construction and Equipment entered into their first contract to obtain supplies from Gold Peak.

14. In March 2020, end-users of Gold Peak products began to notice deficiencies in those products and utilized DoD Product Quality Deficiency Reports (PQDR) to notify DLA. The first PQDR, dated March 26th 2020, was filed by the Letterkenny Army Depot and related to contract SPE8E7-20-V-0581, which was for the purchase of 25 Tubexial Fans, NSN 4140-014-68-8102, at a unit price of \$668 and total price of \$16,700. The PQDR noted the fan was to be installed on a Patriot Missile but found that the received part did not match the specification drawing. The PDQR noted the NSN drawing called for a terminal block but the part provided by Gold Peak had wires instead of a terminal block. DLA conducted a visual inspection of a fan

provided in the order and found that in addition to missing a connector that was called for in the drawing, the part provided by Gold Peak measured 5.551 inches in length and 2.63 inches wide while the NSN requirements had a required length of 4.69 inches and width of 1.5 inches. Military specifications are designed with precise measurements to meet the form, fit, and function of the utilized platforms. Accordingly, nonconforming parts may not be able to be installed, and may be of no use.

15. Another PQDR was completed on April 22nd, 2020 by the U.S. Navy ship USS PRINCETON for a ventilating fan received by Gold Peak pursuant to contract SPE8E7-20-P-0190. The PQDR noted the ordered part was the wrong size and plugged into a wall outlet, which is not called for in the NSN specifications. DLA again tested one of the fans provided by Gold Peak on this contract and found, “The given product was far too big and not the correct item as requested in the drawing.” The following month, May 2020, the USS ROSS completed a PQDR for another fan on the same contract noting, “The fans are not up to specifications for the Spy Radar.” Another PQDR filed by the Red River Army Depot found that a 20” Lasko Home or Office retail fan, which retails for less than \$200 on Amazon, was provided in response to a request for fans to be installed on a Bradley Fighting Vehicle. DLA paid Gold Peak \$1,895 per fan on this contract for a total of \$7580.00.

16. In all, according to the Product Reporting and Evaluation Program Automated Information System (PDREP-AIS) at least 161 PQDRs were filed related to products provided by Gold Peak. Based on my training and experience, I understand that it is common for service members to simply throw away or otherwise utilize non-conforming products, without going through the time-consuming process of submitting a PQDR. Accordingly, it is likely that

additional non-conforming products were provided by Gold Peak, beyond those identified in the PQDRs.

17. Due to the amount of non-conforming product identified through PQDRs DLA Construction and Equipment tested a sampling of items provided by Gold Peak in inventory. Products related to fourteen of those contracts were found not to meet the required specifications. DLA has placed all product that could be identified as provided by Gold Peak in quarantine to mitigate the risk of bad parts being provided to DoD components.

18. On April 22, 2022, your affiant visited the DLA Distribution Center Susquehanna in New Cumberland, PA to view some of the products provided to DLA by Gold Peak. One of the products viewed was a fan purchased under Delivery Order SPE8E7-20-P-1706 which was an order for 6 Circulating Fans, NSN 4140-01-616-1174 at a unit price of \$1445. Gold Peak had indicated in its quote that the fans would meet the NSN specifications and the fans would be obtained from CAGE 39428, which belongs to MCMaster-Carr Supply Company. When your affiant viewed the actual product delivered by Gold Peak, it was a Honeywell TurboForce commercial off-the-shelf fan. The box had been turned inside out before being shipped to DLA and on the inside of the box was a shipping label from Amazon.com to Rena Turner/Gold Peak Industries LLC with an address of 640 Deerfield Dr., Washington PA 15301-9112, Turner's home address. The Honeywell TurboForce fan retails at less than \$100 on Amazon.

19. On June 2nd, 2022, DLA notified Turner that she and Gold Peak were proposed for indefinite debarment from Federal Contracts based on the deficient products identified. On June 22nd, 2022, Turner responded to the proposed debarment and stated that, "In the beginning of 2019, a gentleman approached me from a consulting firm (Smith & Jameson) and offered a 'Service for hire'. The service would be to search for contracts for Gold Peak Industries, LLC to

bid on and if awarded, Mr. Smith would locate the correct material to purchase. Mr. Smith assured me that he had a long-standing working relationship with DLA and his expertise would help Gold Peak and never hinder it. This would eliminate my need for a purchasing agent. When the DLA began sending Quality Notifications in 2020 to present, I realized that Mr. Smith from Smith & Jameson Consulting could not be researching the material needed to satisfy the contract. He stated with each contract that he reviewed the contract and told me what to purchase to satisfy the contract. I cut ties with Smith & Jameson Consulting in 2021 but to my dismay, it was too late. The returns were coming almost daily at first. Presently, I am still receiving returns from 2019 and 2020.” Your affiant reviewed the federal contractors database System for Award Management for Smith & Jamison, which listed the point of contact for the company as Donald Smith. The Articles of Incorporation for Smith & Jamison was signed by Donald Smith, who is listed as the owner. Your affiant is aware of a previous DCIS investigation into Donald Smith for providing DLA with inferior products, which resulted in Smith being debarred by DLA on June 30th 2015.

20. Turner also provided DLA, via her written response, numerous emails between her and DLA procurement or quality personnel. All of those emails utilized the email address Rfiem131@comcast.net. Turner also registered that email address with DLA for communications in the DLA Internet Bid Board System (DIBBS), a system used by DLA and its contractors to solicit and receive bids and award contracts.

21. On February 23rd, 2022, DLA provided your affiant a copy of an email from Turner (using the rfiem131@comcast.net email) to a DLA Acquisition Specialist on December 15th, 2020. Turner’s email was sent in response to a request by DLA to confirm the validity and traceability of product Gold Peak was contracted to deliver in accordance with Contract

SPE8E7-21-P-0487. Turner provided DLA with email correspondence from her vendor for the contract, Amazon.com, in which she utilized rfem131@comcast.net to communicate with the vendor.

22. Based on the foregoing, there is probable cause to believe that Rena Turner utilized rfem131@comcast.net as a primary means of communications while conducting business for Gold Peak, to include communicating with vendors and customers. In addition, Turner likely used the same email address in communicating with consultants such as Smith & Jamison who, according to Turner's statements to DLA, provided guidance to Turner on where to source materials for contracts with DLA.

23. As such, there is probable cause to believe that the email account contains records showing the true source and/or properties of the material Turner provided to DLA, which she misrepresented to DLA. Your affiant therefore requests an order authorizing the seizure of data related to the aforementioned email address.

BACKGROUND CONCERNING EMAIL

24. In general, an email that is sent to a Comcast subscriber is stored in the subscriber's "mail box" on Comcast's servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on Comcast's servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on Comcast's servers for a certain period of time.

25. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of

payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

26. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

27. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute

evidence of the crimes under investigation because the information can be used to identify the account's user or users.

28. As explained herein, information stored in connection with an email account may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculcate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (*e.g.*,

communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

CONCLUSION

29. Based on the forgoing, I request that the Court issue the proposed search warrant.

30. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Comcast. Because the warrant will be served on Comcast, who will then compile the requested records at a time convenient to it, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,

s/ Steven Adams
STEVEN ADAMS
Special Agent
Defense Criminal Investigative Service

Sworn and subscribed to me, by telephone
pursuant to Fed. R. Crim. P. 4.1(b)(2)(A),
this 9th day of January 2023.

HONORABLE PATRICIA L. DODGE
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with Rfiem131@comcast.net that is stored at premises owned, maintained, controlled, or operated by Comcast Corporation, 1800 Bishops Gate Blvd., Mount Laurel, NJ 08054, which accepts service of legal process at LEASubmit@comcast.com.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Comcast Corp. (the “Provider”)

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all emails associated with the account from January 1, 2019 to present, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number).

c. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

The Provider is hereby ordered to disclose the above information to the government within 14 days of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of Title 18 U.S.C. § 1343 (Wire fraud), 18 U.S.C. § 287 (False, fictitious or fraudulent claims) and 18 U.S.C. § 1031 (Major fraud against the United States), those violations involving Rena Turner and occurring after June 12th, 2019, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- (a) All communications with vendors about the purchase of goods, including invoices, receipts, and shipping manifests;
- (b) All communications with Don Smith, and/or Smith and Jamison;
- (c) All communications regarding the sale of goods to the DLA;
- (d) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;
- (e) Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;
- (f) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT TO
FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)**

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Comcast, and my title is _____ . I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Comcast. The attached records consist of _____ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Comcast, and they were made by Comcast as a regular practice; and

b. such records were generated by Comcast's electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Comcast in a manner to ensure that they are true duplicates of the original records; and
2. the process or system is regularly verified by Comcast, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date

Signature